What is claimed is:

1. An encryption apparatus comprising:

a content processor that receives an audio/video stream, performs one or more predetermined processing operations on the audio/video stream, and generates and outputs predetermined data to be used for generating a random number;

a random number generator that receives the predetermined data from the content processor and generates the random number;

an encryption key generator that receives information comprising the random number and generates an encryption key using the information; and

a content encryptor that encrypts the audio/video stream output from the content processor using the encryption key.

2. The encryption apparatus of claim 1, wherein the content processor compresses the received audio/video stream as MPEG video.

3. The encryption apparatus of claim 2, wherein the content processor generates the predetermined data based on statistical features of the audio/video stream that are generated when compressing the received audio/video stream as the MPEG video.

4. The encryption apparatus of claim 3, wherein the statistical features include at least one of color distribution information, motion estimation information, and noise estimation information of a macroblock that

are generated when compressing the received audio/video stream as the MPEG video.

5. The encryption apparatus of claim 1, wherein the content processor generates and outputs the predetermined data to be used to generate the random number, based on motion vector information that is generated during a motion estimation processing operation.

6. The encryption apparatus of claim 5, wherein the predetermined data is a least significant 1 bit of a motion vector that is generated during the motion estimation processing operation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of motion vectors that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

7. The encryption apparatus of claim 1, wherein the content processor generates and outputs the predetermined data to be used to generate the random number, based on the sum of absolute difference information that is generated during a motion estimation processing operation.

8. The encryption apparatus of claim 7, wherein the predetermined data is a least significant 1 bit of the sum of absolute difference information that is generated during the motion estimation processing

operation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of the sum of absolute difference information that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

9. The encryption apparatus of claim 1, wherein the content processor generates predetermined data to be used to generate the random number, based on variance information that is generated during a Motion Compensated-Discrete Cosine Transform processing operation.

10. The encryption apparatus of claim 9, wherein the predetermined data is a least significant 1 bit of variance information that is generated during the Motion Compensated-Discrete Cosine Transform and then stored in a shift register and a plurality of other least significant 1 bits of variance information that are generated subsequently and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

11. The encryption apparatus of claim 1, wherein the random number generator performs a predetermined operation on the predetermined data received from the content processor and the random number, which is

generated by the random number generator using a predetermined algorithm, to generate a new random number.

12. The encryption apparatus of claim 11, wherein the predetermined operation is a Boolean XOR operation.

13. The encryption apparatus of claim 11, wherein the predetermined algorithm is one of a random number generating algorithm using a linear feedback shift register and a Cellular Automata algorithm.

14. The encryption apparatus of claim 1, wherein the encryption key generator receives content identification information, storage identification information, and copy management control bit information in addition to the random number generated by the random number generator and performs a predetermined operation on the random number, the content identification information, the storage identification information, and the copy management control bit information to generate the encryption key.

15. The encryption apparatus of claim 14, wherein the predetermined operation is one of a Boolean XOR operation that is performed on all bits of the random number, the content identification information, the storage identification information, and the copy management control bit information and a Boolean XOR operation that is performed on predetermined random bits of the random number, the content identification information, the

storage identification information, and the copy management control bit information.

16. An apparatus for generating a random number, the apparatus comprising:

a content processor that receives an audio/video stream, and generates and outputs statistical feature information of the audio/video stream; and

a random number generator that receives the statistical feature information and generates a random number using the statistical feature information.

17. The apparatus of claim 16, wherein the statistical feature information is one of motion vector information that is generated during a motion estimation, the sum of absolute difference information that is generated during the motion estimation, and variance information that is generated during a Motion Compensated-Discrete Cosine Transform.

18. The apparatus of claim 16, wherein the statistical feature information are a least significant 1 bit of a motion vector that is generated during the motion estimation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of motion vectors that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

19. The apparatus of claim 16, wherein the statistical feature information are a least significant 1 bit of the sum of absolute difference information that is generated during motion estimation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of the sum of absolute difference information that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

20. The apparatus of claim 16, wherein the statistical feature information are a least significant 1 bit of variance information that is generated during the Motion Compensated-Discrete Cosine Transform and then stored in a shift register and a plurality of other least significant 1 bits of variance information that are generated subsequently and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

21. An encryption method comprising:

receiving an audio/video stream, performing one or more predetermined processing operations on the audio/video stream, and generating and outputting predetermined data to be used for generating a random number;

receiving the predetermined data and generating the random number;

receiving information comprising the random number and generating an encryption key using the information; and

encrypting the audio/video stream, which has undergone the one or more predetermined processing operations, using the encryption key.

22. The encryption method of claim 21, wherein the one or more predetermined processing operations include compressing the received audio/video stream as MPEG video.

23. The encryption method of claim 22, wherein the predetermined data is generated based on at least one of color distribution information, motion estimation information, and noise estimation information of a macroblock, which are statistical features of the audio/video stream that are generated when compressing the received audio/video stream as the MPEG video.

24. The encryption method of claim 21, wherein in the generating and outputting of the predetermined data, the predetermined data to be used for generating the random number is generated and output using at least one of motion vector information that is generated during a motion estimation, the sum of absolute difference information that is generated during the motion estimation, and variance information that is generated during a Motion Compensated-Discrete Cosine Transform.

25. The encryption method of claim 24, wherein in the generating and outputting of the predetermined data, one of a least significant 1 bit of motion vector information that are generated in each macroblock during the motion estimation, a least significant 1 bit of the sum of absolute difference information that are generated in each macroblock during the motion estimation, and a least significant 1 bit of variance information that is generated during a Motion Compensated-Discrete Cosine Transform in each macroblock, is sequentially stored in the shift register, by shifting a shift register of a predetermined size, and output when the generation of the random number is requested.

26. The encryption method of claim 21, wherein the random number is generated by performing a predetermined operation on the predetermined data and a previously generated random number that was generated using a predetermined random number generating algorithm.

27. The encryption method of claim 26, wherein the predetermined random number generating algorithm is one of a random number generating algorithm using a linear feedback shift register and a Cellular Automata algorithm.

28. The encryption method of claim 21, wherein the encryption key is generated by receiving the random number, content identification information, storage identification information, and copy management control

bit information and performing a predetermined operation on the random number, the content identification information, the storage identification information, and the copy management control bit information.

29. The encryption method of claim 28, wherein the predetermined operation is one of a Boolean XOR operation that is performed on all bits of the random number, the content identification information, the storage identification information, and the copy management control bit information and a Boolean XOR operation that is performed on predetermined random bits of the random number, the content identification information, the storage identification information, and the copy management control bit information.

30. A method of generating a random number, the method comprising:

receiving an audio/video stream, and generating and outputting statistical feature information of the audio/video stream; and

receiving the statistical feature information and generating a random number using the statistical feature information.

31. The method of claim 30, wherein the statistical feature information is one of motion vector information that is generated during a motion estimation, the sum of absolute difference information that is generated during the motion estimation, and variance information that is generated during a Motion Compensated-Discrete Cosine Transform.

32. The method of claim 30, wherein the statistical feature information are a least significant 1 bit of a motion vector that is generated during the motion estimation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of motion vectors that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

33. The method of claim 30, wherein the statistical feature information are a least significant 1 bit of the sum of absolute difference information that is generated during motion estimation in a macroblock and then stored in a shift register and a plurality of other least significant 1 bits of the sum of absolute difference information that are generated in subsequent macroblocks and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored least significant 1 bits being output when the generation of the random number is requested.

34. The method of claim 30, wherein the statistical characteristic information are a least significant 1 bit of variance information that is generated during the Motion Compensated-Discrete Cosine Transform and then stored in a shift register and a plurality of other least significant 1 bits of variance information that are generated subsequently and then sequentially stored in the shift register, by shifting the shift register bit by bit, the stored

least significant 1 bits being output when the generation of the random number is requested.

35. A computer-readable recording medium on which a program is recorded to execute the method of claim 21 in a computer.

36. A computer-readable recording medium on which a program is recorded to execute the method of claim 30 in a computer.